*RIMS Kôkyûroku Bessatsu*
**B51** (2014), 139–149

# Higher Fitting ideals of Iwasawa modules and Euler systems

By

Tatsuya Ohshita*

## § 1. Introduction and main results

### § 1.1. Introduction

Iwasawa main conjecture (in a context of general Galois representations) is a problem on Iwasawa theory which attempts to describe the characteristic ideals of certain "arithmetic" Iwasawa modules related to Selmer groups by using "analytic" ideal related to $p$-adic $L$-functions (if exist). However, characteristic ideals are not enough to determine the pseudo-isomorphism classes of Iwasawa modules completely. The higher Fitting ideals have more detailed information on Iwasawa modules. For instance, the higher Fitting ideals determine the pseudo-isomorphism class and the least cardinality of generators of finitely generated torsion Iwasawa modules (cf. Appendix A).

In [Ku], Kurihara studied the higher Fitting ideals of the minus-part of the Iwasawa module of ideal class groups associated with the cyclotomic $\mathbb{Z}_p$-extension of a CM-field $K$ satisfying certain conditions, and obtained a refinement of the minus-part of the Iwasawa main conjecture for totally real number fields. More precisely, he constructed an ascending filtration $\{\Theta_i\}_{i\in\mathbb{Z}_{\geq 0}}$ of Iwasawa algebra called *the higher Stickelberger ideals*, which are defined by analytic objects arising from $p$-adic $L$-functions, and he proved that the higher Fitting ideals coincide with the higher Stickelberger ideals (cf. [Ku] Theorem 1.1). Note that the keys of Kurihara's result are the minus part of Iwasawa main conjecture for totally real number fields and the Euler system of "Gauss sum type" arising from Stickelberger elements.

Received March 31, 2013. Revised August 9, 2013 and October 20, 2013.
2010 Mathematics Subject Classification(s): Primary 11R23. Secondary 11R18.
*Key Words*: *Iwasawa theory, Euler system, higher Fitting ideals, fine Selmer groups.*
This work is supported by Grant-in-Aid for JSPS Fellows (22-2753) from Japan Society for the Promotion of Science.
*Dep. of Math., Kyoto University, Kyoto 606-8502, Japan.
e-mail: ohshita@math.kyoto-u.ac.jp

The higher Fitting ideals of the plus-part of the Iwasawa modules of ideal class groups (in the case when $K$ is abelian over $\mathbb{Q}$) are studied in [Oh2]. In the article [Oh2], by using the Euler system of circular units, we constructed the ascending filtration $\{\mathfrak{C}_i\}_{i\in\mathbb{Z}_{\geq 0}}$ of the Iwasawa algebra, which are analogues of Kurihara's higher Stickelberger ideals, and proved that $\mathfrak{C}_i$ give "upper bounds" and "lower bounds" of the higher Fitting ideals of the plus-part of the Iwasawa module in certains senses. In particular, under certain assumptions, the results in [Oh2] imply that the filtration $\{\mathfrak{C}_i\}_{i\in\mathbb{Z}_{\geq 0}}$ determines the pseudo-isomorphism class of the plus-part of the Iwasawa module, so they can be regarded as a refinement of the plus-part of the Iwasawa main conjecture over $\mathbb{Q}$. (For details, see [Oh2] Theorem 1.1 and Remark 1.3 in this article.) Though the results in [Oh2] do not give complete descriptions of the higher Fitting ideals, they can be regarded as analogues of Kurihara's results for the plus-part.

This article is an announcement of the author's recent results, which is a generalization of results in [Oh2] for general $p$-adic Galois representations with a Rubin-type Euler system. Under certain assumptions, for a given Euler system $\mathbf{c}$ of a lattice $T$ of a $p$-adic Galois representation, we constructed the ideals $\mathfrak{C}_i(\mathbf{c})$ of Iwasawa algebra, which are analogues of Kurihara's higher Stickelberger ideals. Then, we proved that the ideals $\mathfrak{C}_i(\mathbf{c})$ give "upper bounds" and "lower bounds" of the higher Fitting ideals of a certain Iwasawa module $X(T)$ arising from the lattice $T$. In particular, under the assumption of the "Iwasawa main conjecture" for the pair $(T,\mathbf{c})$, the ideals $\mathfrak{C}_i(\mathbf{c})$ determine the pseudo-isomorphism class of $X(T)$. See Theorem 1.3 and Corollary 1.4 for the precise statements of our main results, and see §2.2 for the construction of the ideal $\mathfrak{C}_i(\mathbf{c})$. Our results also can be regarded as analogues of Kurihara's results in [Ku] and a refinement of "Iwasawa main conjectures" for Rubin type Euler systems.

## § 1.2. Notation

Let $K$ be a field, and fix a separable closure $\overline{K}$ of $K$. Then, we put $G_K := \mathrm{Gal}(\overline{K}/K)$. For a topological abelian group $M$ with a continuous $G_K$-action, let $H^*(K,M) = H^*(G_K,M)$ be the continuous Galois cohomology group.

Let $\ell$ be a prime number. We denote by $W_{\mathbb{Q}_\ell}$ the Weil group of $\mathbb{Q}_\ell$, and by $I_{\mathbb{Q}_\ell} = G_{\mathbb{Q}_\ell^{\mathrm{ur}}}$ the inertia subgroup of $W_{\mathbb{Q}_\ell}$.

In this paper, an algebraic number field $K$ is a finite extension of $\mathbb{Q}$ in this fixed algebraic closure $\overline{\mathbb{Q}}$. We denote the ring of integers $K$ by $\mathcal{O}_K$. For any positive integer $n$, let $\mu_n := \boldsymbol{\mu}_n(\overline{\mathbb{Q}})$ be the group of $n$-th roots of unity in $\overline{\mathbb{Q}}$.

Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, and let $c \in G_{\mathbb{Q}}$ be the complex conjugation corresponding to this embedding. For any abelian group $M$ with action of $G_{\mathbb{Q}}$, we denote by $M^-$ the subgroup of $M$ consisting of all elements on which $c$ acts via $-1$.

Let $R$ be a commutative ring, and $M$ an $R$-module. For any $a \in R$, let $M[a]$ be the $R$-submodule of $M$ consisting of all $a$-torsion elements. We denote the ideal of $R$

consisting of all annihilators of $M$ by $\mathrm{Ann}_R(M)$.

Let $G$ be a group, and $M$ an abelian group with an action of $G$. Then, we denote by $M^G$ the maximal subgroup of $M$ fixed by the action of $G$.

## § 1.3. Main results

Fix an odd prime number $p$. Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension. For any $m \in \mathbb{Z}_{\geq 0}$, let $\mathbb{Q}_m$ be the unique intermediate field of $\mathbb{Q}_\infty/\mathbb{Q}$ satisfying $[\mathbb{Q}_m : \mathbb{Q}] = p^m$. We put $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, and define a compact local algebra $\Lambda$ by

$$\Lambda := \mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})].$$

Let $\Sigma$ be a finite set of places of $\mathbb{Q}$ containing $\{p, \infty\}$, and $T$ a free $\mathbb{Z}_p$-module of finite rank $d$ with a continuous action of $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ unramified outside $\Sigma$. We denote the action of $G_\mathbb{Q}$ on $T$ by

$$\rho_T \colon G_\mathbb{Q} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T) \simeq \mathrm{GL}_d(\mathbb{Z}_p).$$

We regard $T$ as an étale pro-$p$ sheaf on $\mathrm{Spec}\mathcal{O}_{\mathbb{Q}_m,\Sigma}$, where $\mathcal{O}_{\mathbb{Q}_m,\Sigma}$ is the ring of $\Sigma$-integers of $\mathbb{Q}_m$. We put $A := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$, and $A^* := \mathrm{Hom}(T, \mu_{p^\infty})$. In this article, we assume the following conditions.

(C1) The representation $A[p]$ of $G_{\mathbb{Q}_\infty}$ over $\mathbb{F}_p$ is absolutely irreducible.

(C2) There exists an element $\tau \in G_{\mathbb{Q}(\mu_{p^\infty})}$ such that $T/(\tau - 1)T$ is a free $\mathbb{Z}_p$-module of rank one.

(C3) The $\mathbb{F}_p[G_{\mathbb{Q}_\infty}]$-module $A[p]$ is *not* isomorphic to $A^*[p]$.

(C4) If the rank of $A$ is one, then $G_{\mathbb{Q}_\infty}$ does not act on $A[p]$ via the trivial character $\mathbf{1}$ or Teichmüller character $\omega$.

(C5) Let $\Omega = \mathbb{Q}(\mu_p^\infty, A)$ be the maximal subfield of $\overline{\mathbb{Q}}$ fixed by the action of

$$\ker\left(G_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathrm{Aut}(A)\right).$$

Then, we have

$$H^1(\Omega/\mathbb{Q}_\infty, A) = H^1(\Omega/\mathbb{Q}_\infty, A^*) = 0.$$

(C6) The torsion $\mathbb{Z}_p$-module $H^0_{\text{ét}}(\mathbb{Q}_\infty \otimes_\mathbb{Q} \mathbb{Q}_p, A^*)$ is divisible.

(C7) Let $\ell \in \Sigma \setminus \{p, \infty\}$ be any element. Let

$$(r_\ell \colon W_{\mathbb{Q}_\ell} \longrightarrow \mathrm{GL}_d(\mathbb{Q}_p), N_\ell)$$

be the Weil-Deligne representation corresponding to $(T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \rho_T|_{W_{\mathbb{Q}_\ell}})$. Then, the following holds.

(i) The prime number $p$ does not divide $\#r_\ell(I_{\mathbb{Q}_\ell}) = [L_\ell : \mathbb{Q}_\ell^{\mathrm{ur}}]$.

(ii) The $\mathbb{Z}_p$-module $H^1_{\mathrm{cont}}(G_{L_\ell}, T)$ is torsion free.

We can prove the following lemma which gives a sufficient condition for the condition (ii) of (C7).

**Lemma 1.1.** *Let $\ell \in \Sigma \setminus \{p, \infty\}$ be any element. We let $(r_\ell, N_\ell)$ and $L_\ell$ be as in (C7). Fix a topological generator $g_\ell$ of the tame inertia group $I^t_{L_\ell}$ of $L_\ell$. Suppose that the $\mathbb{Z}_p$-module the $\mathbb{Z}_p$-module $T/(g_\ell - 1)T$ is torsion free. Then, the $\mathbb{Z}_p$-module $H^1_{\mathrm{cont}}(I_{L_\ell}, T)$ is torsion free.*

**Definition 1.2.** Let $j\colon \mathrm{Spec}\mathcal{O}_{\mathbb{Q}_m,\Sigma} \hookrightarrow \mathrm{Spec}\mathcal{O}_{\mathbb{Q}_m}[1/p]$ be the inclusion. We put

$$\mathbb{H}^i(T) := \varprojlim H^i_{\text{ét}}(\mathcal{O}_{\mathbb{Q}_m}[1/p], j_*T),$$
$$\mathbb{H}^i_{\mathrm{loc}}(T) := \varprojlim H^i_{\text{ét}}(\mathbb{Q}_m \otimes_{\mathbb{Q}} \mathbb{Q}_p, j_*T).$$

Then, we define

$$X(T) := \ker\left(\mathbb{H}^2(T) \longrightarrow \mathbb{H}^2_{\mathrm{loc}}(T)\right).$$

We denote the maximal pseudo-null $\Lambda$-submodule of $X(T)$ by $X_{\mathrm{fin}}(T)$.

We write $X := X(T)$ and $X_{\mathrm{fin}} := X_{\mathrm{fin}}(T)$ for simplicity. Note that $X$ is a $\Lambda$-module which is isomorphic to the Pontrjagin dual of the "fine Selmer group" $\mathcal{S}_{\Sigma_p}(\mathbb{Q}_\infty, A^*)$ in the sense of [Ru] Definition 2.3.1. It is well-known that $X$ is a finitely generated $\Lambda$-module. In this article, we study the higher Fitting ideals of the $\Lambda$-module $X' := X/X_{\mathrm{fin}}$ under the assumption of the existence of an Euler system for $T$ satisfying the "non-vanishing condition" (NV) explained below.

In order to mention Euler systems, we need to introduce some abelian extension fields of $\mathbb{Q}$. For each prime number $\ell$ not contained in $\Sigma$, we denotes by $\mathbb{Q}(\ell)$ by the maximal subfield of $\mathbb{Q}(\mu_p)$ whose extension degree over $\mathbb{Q}$ is a $p$-power. Let $\mathcal{N}(\Sigma)$ be the set of all positive integers decomposed into square free products of prime numbers not contained in $\Sigma$. Here, we promise $1 \in \mathcal{N}(\Sigma)$. Let $n \in \mathcal{N}(\Sigma)$ be any element, and assume that $n$ has a prime factorization $n = \prod_{i=1}^r \ell_i$. Then, we define the composite field

$$\mathbb{Q}_m(n) := \mathbb{Q}_m\mathbb{Q}(\ell_1)\cdots\mathbb{Q}(\ell_r)$$

for any $m \geq 0$.

In this paper, we assume that there exists an Euler system

$$\mathbf{c} := \left\{c_m(n) \in H^1(\mathbb{Q}_m(n), T)\right\}_{m\geq 0, n\in\mathcal{N}(\Sigma)}$$

in the sense of [Ru] Remark 2.1.4 satisfying the following "non-vanishing condition":

(NV) The element $\mathbf{c}(1) := (c_m(1))_{m\geq 0} \in \mathbb{H}^1(T)$ is not $\Lambda$-torsion.

We define the ideal $\mathrm{Ind}(\mathbf{c})$ of $\Lambda$ by

$$\mathrm{Ind}(\mathbf{c}) := \left\{ \varphi\left(\mathbf{c}(1)\right) \mid \varphi \in \mathrm{Hom}_\Lambda\left(\mathbb{H}^1(j_*T), \Lambda\right) \right\},$$

and denote by $\mathrm{pInd}(\mathbf{c})$ the minimal principal ideal of $\Lambda$ containing $\mathrm{Ind}(\mathbf{c})$. By usual Euler system arguments, the assumption (NV) implies that $X$ is a torsion $\Lambda$-module, and we have

$$\mathrm{char}_\Lambda(X) \supseteq \mathrm{pInd}(\mathbf{c}), \tag{1.1}$$

where $\mathrm{char}_\Lambda(X)$ is the characteristic ideal of the $\Lambda$-module $X$. (See Theorem 2.3.2 and Theorem 2.3.3 in [Ru].) We define the ideal $I_\varphi(\mathbf{c})$ of $\Lambda$ by

$$I_\varphi(\mathbf{c}) := \{a \in \Lambda \mid a \cdot \mathrm{char}_\Lambda(X) \subseteq \varphi(\mathbf{c}(1)) \cdot \Lambda\}$$

for any homomorphism $\varphi \in \mathrm{Hom}_\Lambda\left(\mathbb{H}^1(j_*T), \Lambda\right)$, and put

$$I(\mathbf{c}) := \bigcup_{\varphi \in \mathrm{Hom}_\Lambda(\mathbb{H}^1(j_*T), \Lambda)} I_\varphi(\mathbf{c}).$$

(Note that $I(\mathbf{c})$ is an ideal of $\Lambda$.) By the definition of $I(\mathbf{c})$ and (1.1), we have

$$\mathrm{Ind}(\mathbf{c}) = I(\mathbf{c}) \cdot \mathrm{char}_\Lambda(X). \tag{1.2}$$

Under the assumption (NV), we sometimes consider the following condition (MC), which is "Iwasawa main conjecture" for $(T, \mathbf{c})$.

(MC) The characteristic ideal of the $\Lambda$-module $X$ coincides with $\mathrm{Ind}(\mathbf{c})$, that is, we have

$$\mathrm{char}_\Lambda(X) = \mathrm{pInd}(\mathbf{c}).$$

Note that if $\mathbb{H}^1(j_*T)$ is generically rank one over $\Lambda$, namely we have

$$\dim_{\mathrm{Frac}(\Lambda)} \mathbb{H}^1(j_*T) \otimes_\Lambda \mathrm{Frac}(\Lambda) = 1,$$

and if the condition (MC) holds, then $I(\mathbf{c}) = \Lambda$.

In order to state our main theorem, it is convenient to introduce the following notation. Let $I$ and $J$ be ideals of $\Lambda$. We write $I \prec J$ if there exists a height two ideal $\mathcal{A}$ of $\Lambda$ (called an "error factor") satisfying $\mathcal{A}I \subseteq J$. Note that for two ideals $I$ and $J$ of $\Lambda$, we have $I \prec J$ if and only if $I\Lambda_\mathfrak{p} \subseteq J\Lambda_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of height one, where we denote the localization of $\Lambda$ at $\mathfrak{p}$ by $\Lambda_\mathfrak{p}$. We write $I \sim J$ if $I \prec J$ and $J \prec I$. The relation $\sim$ is an equivalence relation on ideals of $\Lambda$.

A key idea of our results lies in the definition of the ideals $\mathfrak{C}_i(\mathbf{c})$ of $\Lambda$, which are analogues of Kurihara's higher Stickelberger ideals. We define such ideals in §2 by using Kolyvagin derivatives of the Euler system $\mathbf{c}$. Roughly speaking, first, we define the ideals $\mathfrak{C}_{i,m,N}(\mathbf{c})$ of the group ring $R_{m,N} := \mathbb{Z}/p^N[\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})]$ generated by images of certain Kolyvagin derivatives $\kappa_{m,N}(n;\mathbf{c})$ by *all* $R_{m,N}$*-homomorphisms*

$$H^1(\mathbb{Q}_m, T/p^N T) \longrightarrow R_{m,N},$$

then we define $\mathfrak{C}_i(\mathbf{c})$ by taking the projective limit of them. (For details, see Definition 2.5 and Definition 2.7). The following theorem is the main results of this article.

**Theorem 1.3** ([Oh3])**.** *Let $T$ and $\mathbf{c}$ be as above. Especially, we assume the hypotheses* (C1)–(C7) *and* (NV)*. Then, the following holds.*

1. *For any $i \in \mathbb{Z}_{\geq 0}$, we have*

$$\mathrm{Ann}_\Lambda(X_{\mathrm{fin}}) I(\mathbf{c}) \cdot \mathrm{Fitt}_{\Lambda,i}(X') \subseteq \mathfrak{C}_i(\mathbf{c}).$$

2. *Assume that $T^-$ is a free $\mathbb{Z}_p$-module of rank one. Then, for any $i \in \mathbb{Z}_{\geq 0}$, we have*

$$\mathfrak{C}_i(\mathbf{c}) \prec \mathrm{Fitt}_{\Lambda,i}(X).$$

*Idea of proof.* The first assertion of Theorem 1.3 for $i = 0$ follows from the comparison between $\mathrm{Ind}(\mathbf{c})$ and $\mathfrak{C}_0(\mathbf{c})$.

The projective dimension of the $\Lambda$-module $X'$ is one since $X'$ has no non-trivial pseudo-null $\Lambda$-submodule. So, we have a free resolution

$$0 \longrightarrow \Lambda^r \xrightarrow{f} \Lambda^r \longrightarrow X' \longrightarrow 0 \tag{1.3}$$

for some positive integer $r$. We apply (a modified version of) "Kurihara's Euler system arguments" to the exact sequence (1.3): we approximate minors of the square matrix corresponding to the $\Lambda$-linear map $f$ by using Kolyvagin derivatives. (Strictly speaking, we cannot apply Kurihara's Euler system arguments in [Ku] directly to our framework since the "fine Selmer group" $\mathcal{S}_{\Sigma_p}(\mathbb{Q}_m, A^*)$ may have infinite order in general, and since we do not have a free $\mathbb{Z}_p$-module as "$\mathrm{Div}(\mathcal{O}_{\mathbb{Q}_m}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$". But after certain modifications, Kurihara's arguments work in our situation.) Then, we obtain the first assertion for $i > 0$. Note that the hypothesis (C3) and the equality (1.2) play essential roles in Kurihara's Euler system arguments.

The key of the second assertion is the comparison between $\mathfrak{C}_i(\mathbf{c})$ and the theory of Kolyvagin systems, which is established by Mazur and Rubin ([MR]). □

By theorem 1.3, we immediately obtain the following corollaries.

**Corollary 1.4.** *Assume that $T$ and $\mathbf{c}$ satisfy hypotheses* (C1)–(C7), (NV) *and* (MC). *We also assume that $T^-$ is a free $\mathbb{Z}_p$-module of rank one. Then, we have*

$$\mathrm{Fitt}_{\Lambda,i}(X) \sim \mathfrak{C}_i(\mathbf{c})$$

*for any $i \in \mathbb{Z}_0$. In other words, the ascending filtration $\{\mathfrak{C}_i(\mathbf{c})\}_{i\in\mathbb{Z}_{\geq 0}}$ of $\Lambda$ determines the pseudo-isomorphism class of $X$.*

*Remark* (circular units). Let $K/\mathbb{Q}$ be an abelian extension satisfying $p \nmid [K:\mathbb{Q}]$ and unramified at $p$. We put $\Delta := \mathrm{Gal}(K\mathbb{Q}(\mu_p)/\mathbb{Q})$, and fix an even character $\chi \in \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times)$ satisfying $\chi|_{G_{\mathbb{Q}_p}} \neq 1$. We define a $\mathbb{Z}_p[G_\mathbb{Q}]$-module $T_\chi$ by

$$T_\chi := \mathbb{Z}_p(1) \otimes \chi^{-1}.$$

For any $m \in \mathbb{Z}_{\geq 0}$, let $A_{m,\chi}$ be the $\chi$-part of the $p$-Sylow subgroup of the ideal class group of $K\mathbb{Q}(\mu_{p^{m+1}})$, and define a $\Lambda$-module $X_\chi$ by $X_\chi := \varprojlim A_{m,\chi}$. Then, we have a natural isomorphism $X_\chi \simeq X(T_\chi)$ of $\Lambda$-modules. Note that $\mathbb{Z}_p(1)\otimes\chi^{-1}$ satisfies (C1)–(C6), and we have an Euler system $\mathbf{c}_\chi^{\mathrm{cyc}}$ of "circular units" for $\mathbb{Z}_p(1)\otimes\chi^{-1}$ satisfying (NV) and (MC). So we can apply Theorem 1.3 to the pair $(T_\chi, \mathbf{c}_\chi^{\mathrm{cyc}})$, and obtain $\mathrm{Fitt}_{\Lambda,i}(X_\chi) \sim \mathfrak{C}_i(\mathbf{c}_\chi^{\mathrm{cyc}})$ and

$$\mathrm{Ann}_\Lambda(X_{\chi,\mathrm{fin}}) \cdot \mathrm{Fitt}_{\Lambda,i}(X'_\chi) \subseteq \mathfrak{C}_i(\mathbf{c}_\chi^{\mathrm{cyc}})$$

for any $i \geq 0$. This is the result we obtained in Theorem 1.1 in [Oh2]. Moreover, in this case, we can prove the following statements:

- The least cardinality of generators of the $\Lambda$-module $X_\chi$ is $r$ if and only if we have $\mathfrak{C}_{r-1}(\mathbf{c}_\chi^{\mathrm{cyc}}) \neq \Lambda$ and $\mathfrak{C}_r(\mathbf{c}_\chi^{\mathrm{cyc}}) = \Lambda$.
- If the $\Lambda$-module $X$ is pseudo-null, then we have

$$\mathrm{Fitt}_{\Lambda,0}(X_\chi) = \mathrm{Ann}_\Lambda(X_\chi) = \mathfrak{C}_0(\mathbf{c}_\chi^{\mathrm{cyc}}).$$

For details of such results on circular units, see [Oh2]. Note that we also treat an arbitrary non-trivial character $\chi \in \mathrm{Hom}(\Delta, \overline{\mathbb{Q}}_p^\times)$ in [Oh2].

*Remark* (elliptic units). For the Iwasawa modules of ideal class groups associated with (not necessary cyclotomic) $\mathbb{Z}_p$-extensions of a certain abelian extension field of an imaginary quadratic field and Euler systems of elliptic units, we have similar results to the first and second assertions of Theorem 1.3. For details, see [Oh1] Theorem 1.1.

## § 2. Construction of the ideal $\mathfrak{C}_i(\mathbf{c})$

In this section, we construct the filtration $\{\mathfrak{C}_i\}$ of $\Lambda$. Here, we use similar notations to that in §1. In particular, we let $T$ and $\mathbf{c}$ be as in Theorem 1.3. For a while, we fix integers $m$ and $N$ satisfying $N > m \geq 0$.

## § 2.1. Kolyvagin derivatives

First, we recall the notion of Kolyvagin derivatives briefly. We define a set $\mathcal{P}_N(\Sigma;T)$ of prime numbers by

$$\mathcal{P}_N(\Sigma;T) := \left\{ \ell \;\middle|\; \begin{array}{l} \ell \notin \Sigma,\ \ell \equiv 1 \bmod p^N, \text{ and } T/(p^N T + (\mathrm{Fr}_\ell - 1)T) \text{ is} \\ \text{a free } \mathbb{Z}_p/p^N\mathbb{Z}_p\text{-module of rank one} \end{array} \right\},$$

where $\mathrm{Fr}_\ell \in G_{\mathbb{Q}}$ is an arithmetic Frobenius element at $\ell$. Then, we put

$$\mathcal{N}_N(\Sigma;T) := \left\{ \prod_{i=1}^{r} \ell_i \;\middle|\; \begin{array}{l} r \in \mathbb{Z}_{>0},\ \ell_i \in \mathcal{P}_N(\Sigma;T)\ (i=1,\dots,r) \\ \text{and } \ell_i \neq \ell_j \text{ if } i \neq j \end{array} \right\} \cup \{1\}.$$

For simplicity, we write $\mathcal{P}_N := \mathcal{P}_N(\Sigma;T)$ and $\mathcal{N}_N := \mathcal{N}_N(\Sigma;T)$. We define $H_n := \mathrm{Gal}\,(\mathbb{Q}(n)/\mathbb{Q})$ for any $n \in \mathcal{N}_N$. If $n$ is decomposed as $n = \prod_{i=1}^{r} \ell_i$, where $\ell_1, \dots, \ell_r$ are distinct prime numbers, then we have natural isomorphisms

$$\mathrm{Gal}(\mathbb{Q}_m(n)/\mathbb{Q}_m) \simeq H_n \simeq H_{\ell_1} \times \cdots \times H_{\ell_r}$$

for any integer $m \geq 0$. We identify these groups by the above natural isomorphisms.

**Definition 2.1.** For $\ell \in \mathcal{P}_N$, we define

$$D_\ell := \sum_{k=1}^{\ell-2} k\sigma_\ell^k \in \mathbb{Z}[H_\ell].$$

Let $n = \prod_{i=1}^{r} \ell_i \in \mathcal{N}_N$, where $\ell_i \in \mathcal{P}_N$ for each $i$. Then, we define

$$D_n := \prod_{i=1}^{r} D_{\ell_i} \in \mathbb{Z}[H_n].$$

**Lemma 2.2** ([Ru] Lemma 4.4.2)**.** *For any $n \in \mathcal{N}_N$, the image of $D_n c_m(n)$ in $H^1(\mathbb{Q}_m(n), T/p^N T)$ is fixed by the action of $H_n$.*

Note that the assumptions (C1) and (C4) imply that

$$H^0(\mathbb{Q}_m(n), T/p^N T) = H^0(\mathbb{Q}_m, T/p^N T) = 0$$

for any $n \in \mathcal{N}_N$. So, by Hochschild–Serre spectral sequence, we have a natural isomorphism

$$H^1(\mathbb{Q}_m, T/p^N T) \xrightarrow{\simeq} H^1(\mathbb{Q}_m(n), T/p^N T)^{H_n}.$$

**Definition 2.3.** Let $n$ be any element of $\mathcal{N}_N$. We denote by $\kappa_{m,N}(n;\mathbf{c})$ the unique element of $H^1(\mathbb{Q}_m, T/p^N T)$ whose image in $H^1(\mathbb{Q}_m(n), T/p^N T)$ coincides with that of $D_n c_m(n)$. The cohomology class $\kappa_{m,N}(n;\mathbf{c})$ is called *Kolyvagin derivative*.

## § 2.2. Construction of the ideal $\mathfrak{C}_i(\mathbf{c})$

Here, let us construct the ideal $\mathfrak{C}_i(\mathbf{c})$ of $\Lambda$. Recall that we put

$$R_{m,N} := \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})].$$

First, we construct an ascending filtration $\{\mathfrak{C}_{i,m,N}(\mathbf{c})\}_{i\in\mathbb{Z}_{\geq 0}}$ of $R_{m,N}$. As in [Ku], we need the notion of *well-ordered* integers.

**Definition 2.4.** Let $n \in \mathcal{N}_N$. We call $n$ *well-ordered* if $n$ has a factorization $n = \prod_{i=1}^{r} \ell_i$ with $\ell_i \in \mathcal{P}_N$ such that $\ell_{i+1}$ splits in $\mathbb{Q}_m\big(\mu_{\prod_{j=1}^{i}\ell_j}\big)/\mathbb{Q}$ for any $i$ satisfying $1 \leq i \leq r-1$. In other words, $n$ is well-ordered if and only if $n$ has a factorization $n = \prod_{i=1}^{r} \ell_i$ such that

$$\ell_{i+1} \equiv 1 \pmod{p^N \prod_{j=1}^{i} \ell_j}$$

for $i = 1, \ldots, r-1$. We denote by $\mathcal{N}_N^{\mathrm{w.o.}}$ the set of all elements in $\mathcal{N}_N$ which are well-ordered.

Let $n \in \mathcal{N}_N^{\mathrm{w.o.}}$ with the decomposition $n = \prod_{i=1}^{r} \ell_i$, where $\ell_i \in \mathcal{P}_N$ for each $i$. We put $\epsilon(n) := r$. Namely, $\epsilon(n)$ is the number of prime divisors of $n$. We define the ideal $\mathfrak{C}_{m,N}(n)$ of $R_{m,N}$ by

$$\mathfrak{C}_{m,N}(n;\mathbf{c}) := \left\{ f(\kappa_{m,N}(n;\mathbf{c})) \mid f \in \mathrm{Hom}_{R_{m,N}}(H^1(\mathbb{Q}_m, T/p^N T), R_{m,N}) \right\}.$$

**Definition 2.5.** Let $i$ be a non-negative integer. Then, we denote by $\mathfrak{C}_{i,m,N}(\mathbf{c})$ the ideal of $R_{m,N}$ generated by $\bigcup_n \mathfrak{C}_{m,N}(n;\mathbf{c})$ where $n$ runs through all elements of $\mathcal{N}_N^{\mathrm{w.o.}}$ satisfying $\epsilon(n) \leq i$.

Now vary $m$ and $N$, and let us construct the ideal $\mathfrak{C}_i(\mathbf{c})$ of $\Lambda$. As in [Oh1] Claim 4.4, the following lemma holds.

**Lemma 2.6.** *Let $m_1$, $m_2$, $N_1$ and $N_2$ be positive integers satisfying $m_2 \geq m_1$ and $N_2 \geq N_1$. Take any element $n \in \mathcal{N}_{N_2}$. Then, For any $R_{m_2,N_2}$-homomorphism*

$$f_2 \colon H^1(\mathbb{Q}_{m_2}, T/p^{N_2}T) \longrightarrow R_{m_2,N_2},$$

*there exists an $R_{m_1,N_1}$-homomorphism*

$$f_1 \colon H^1(\mathbb{Q}_{m_1}, T/p^{N_1}T) \longrightarrow R_{m_1,N_1},$$

*which makes the diagram*

$$\begin{array}{ccc} H^1(\mathbb{Q}_{m_2}, T/p^{N_2}T) & \xrightarrow{f_2} & R_{m_2,N_2} \\ \Big\downarrow{\scriptstyle N_{F_{m_2}/F_{m_1}}} & & \Big\downarrow \\ H^1(\mathbb{Q}_{m_1}, T/p^{N_1}T) & \xrightarrow{f_1} & R_{m_1,N_1} \end{array}$$

*commute, where the left vertical arrow $N_{F_{m_2}/F_{m_1}}$ is the corestriction map, and the right one is the natural projection.*

Let $m_1, m_2, N_1, N_2$ and $n$ be as above, and assume $N_i > m_i$ for each $i = 1, 2$. Then, Lemma 2.6 and the "norm compatibility" of the Euler system $\mathbf{c}$ imply that the image of $\mathfrak{C}_{m_2,N_2}(\mathbf{c})$ in $R_{m_1,N_1}$ is contained in $\mathfrak{C}_{m_1,N_1}(\mathbf{c})$. We obtain the projective system of the natural homomorphisms

$$\left\{\mathfrak{C}_{i,m_2,N_2}(\mathbf{c}) \longrightarrow \mathfrak{C}_{i,m_1,N_1}(\mathbf{c}) \;\middle|\; N_2 \geq N_1 > m_1 \text{ and } N_2 > m_2 \geq m_1.\right\}$$

We define $\mathfrak{C}_i(\mathbf{c})$ as follows.

**Definition 2.7.** Let $i$ be a non-negative integer. Then ideal $\mathfrak{C}_i(\mathbf{c})$ of $\Lambda = \varprojlim R_{m,N}$ is defined by the projective limit

$$\mathfrak{C}_i(\mathbf{c}) := \varprojlim \mathfrak{C}_{i,m,N}(\mathbf{c}).$$

## § Appendix A. Higher Fitting ideals

In this appendix, we recall the definition and some basic properties of higher Fitting ideals.

**Definition Appendix A.1.** Let $R$ be a commutative ring, and $M$ be a finitely presented $R$-module. Let

$$R^m \xrightarrow{f} R^n \longrightarrow M \longrightarrow 0$$

be an exact sequence of $R$-modules. For each $i \geq 0$, we define *the $i$-th Fitting ideal* $\mathrm{Fitt}_{R,i}(M)$ to be the ideal of $R$ generated by all $(n-i) \times (n-i)$ minors of the matrix corresponding to $f$. Note that when $0 \leq i < n$ and $m < n - i$ (resp. $i \geq n$), we define $\mathrm{Fitt}_{R,i}(M) := 0$ (resp. $\mathrm{Fitt}_{R,i}(M) := R$). Definition of these ideals depends only on $M$, and does not depend on the choice of the above exact sequence. We have the ascending filtration

*Remark.* Let $R$ be a commutative ring, $S$ a commutative $R$-algebra, and $M$ a finitely presented $R$-module, Then, by the definition of the higher Fitting ideals and the right exactness of tensor products, we have

$$\mathrm{Fitt}_{S,i}(M \otimes_R S) = \mathrm{Fitt}_{R,i}(M)S$$

for any $i \geq 0$.

*Remark.* Let $R$ be a commutative ring, and $M$ a finitely presented $R$-module. If we have $\mathrm{Fitt}_{R,i}(M) \neq R$, then the least cardinality of generators of $M$ is greater than $i + 1$. Note that when $R$ is a local ring or a PID, the least cardinality of generators of $M$ is $i + 1$ if and only if $\mathrm{Fitt}_{R,i}(M) \neq R$ and $\mathrm{Fitt}_{R,i+1}(M) = R$.

*Remark.* Here we assume $R = \Lambda$. Let $M$ and $N$ be $\Lambda$-modules. We say that $M$ is *pseudo-null* if the order of $M$ is finite. We write $M \sim_{\mathrm{p.i.}} N$ if there exists a homomorphism $M \longrightarrow N$ whose kernel and cokernel are both pseudo-null. We call $M$ is *pseudo-isomorphic* to $N$. Note the relation $\sim_{\mathrm{p.i.}}$ is an equivalence relation on finitely generated torsion $\Lambda$-modules. In particular, if we assume

$$M \sim_{\mathrm{p.i.}} \bigoplus_{i=1}^{n} \Lambda/f_i\Lambda,$$

where $\{f_i\}_{i=1}^n$ is a sequence of non-zero elements of $\Lambda$ satisfying $f_i \mid f_{i+1}$, then we have

$$\mathrm{Fitt}_{\Lambda,i}(M) \sim \begin{cases} \left(\prod_{k=1}^{n-i} f_k\right)\Lambda & (\text{if } i < n) \\ \Lambda & (\text{if } i \geq n) \end{cases}$$

for any non-negative integer $i$ (cf. [Ku] Lemma 8.2). This implies that the pseudo-isomorphism class of $M$ is determined by the higher Fitting ideals $\{\mathrm{Fitt}_{\Lambda,i}(M)\}_{i\geq 0}$. Note that the characteristic ideal $\mathrm{char}_\Lambda(M)$ is an ideal of $\Lambda$ defined by

$$\mathrm{char}_\Lambda(M) = \left(\prod_{k=1}^{n} f_k\right)\Lambda.$$

So, the characteristic ideal $\mathrm{char}_\Lambda(M)$ is the minimal principal ideal of $\Lambda$ containing $\mathrm{Fitt}_{\Lambda,0}(M)$.

## References


[Ku] Kurihara, M., *Refined Iwasawa theory and Kolyvagin systems of Gauss sum type*, Proceedings of the London Mathematical Society (3) **104** (2012), 728–769.

[MR] Mazur, B. and Rubin, K., *Kolyvagin systems*, Memoirs of the AMS, vol. 168, number 799 (2004).

[No] Northcott, D. G., *Finite free resolutions*, Cambridge Univ. press (1976).

[Oh1] Ohshita, T., *On higher Fitting ideals of Iwasawa modules of ideal class groups over imaginary quadratic fields and Euler systems of elliptic units*, Kyoto Journal of Mathematics **53** (4) (2013), 713–890.

[Oh2] Ohshita, T., *On the higher Fitting ideals of Iwasawa modules of ideal class groups over real abelian fields*, Journal of Number Theory **135** (2014), 67–138.

[Oh3] Ohshita, T., *On higher Fitting ideals of certain Iwasawa modules associated with Galois representations and Euler systems*, in preparation.

[Ru] Rubin, K., *Euler systems*, Hermann Weyl lectures, Ann. of Math. Studies, vol. 147, Princeton Univ. Press (2000).